The Olive Tree Primary School Bolton

E-Safety POLICY

F Y Choudry

Z Patel

February 2017

Scope of the Policy

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school*:

Governors:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. The Governors receiving regular information about online incidents and monitoring reports will carry this out.

- *All reports and monitoring shared with Governing body when the School deems necessary during Safeguarding, Health and Wellbeing and Computing Meetings.*

Headteacher / Senior Leaders:

The *Principal* has a duty of care for ensuring the safety (including Online) of members of the school community, though the day-to-day responsibility for Online will be delegated to the *Computing Lead.*

- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff.
- *The HeadTeacher/Senior Leaders are responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.*

- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*

- **Computing Lead & Safeguarding Lead:**

• takes day to day responsibility for Online issues and has a leading role in establishing and Reviewing the school online policies / documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.

• provides training and advice for staff

• liaises with school technical staff

• receives reports of online incidents and creates a log of incidents to inform future Online developments,

• meets regularly with Online *Governor* to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting / committee of *Governors*

• reports regularly to Senior Leadership Team

Network Manager - Computeam:

The *Computeam / Computing Lead* ensures:

• The school's technical infrastructure is secure and is not open to misuse or malicious attack

• School meets required online technical requirements and Local Authority requirements addressed.

• Users only access the networks and devices through a properly enforced

password protection policy, in which passwords are regularly changed

• the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (Computeam Computing Lead and Safeguarding Lead)

• Use of the network/internet/ iTunes U Discussions/Showbie/Email/remote access/email is regularly monitored so misuse/attempted misuse can be reported to the Head teacher / Senior Leader; Computing subject leader for investigation / action / sanction

• The Barracuda Filtering solution monitors all online activities.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current *school*

  Online policy and practices.

- they have read, understood and signed the Staff Acceptable Use Policy (AUP)

- they report any suspected misuse or problem to the *Headteacher / Senior Leader Computing Lead/ Safeguarding Lead* for investigation / action / sanction

- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*

- Online issues are embedded in all aspects of the curriculum and other activities

- students / pupils understand and follow the Online and acceptable use policies

- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- *in lessons where internet use is pre-planned students / pupils should be guided to site checked as suitable for their use and that processes are in place for dealing with and unsuitable material that is found in internet searches*

Child Protection / Designated Safeguarding Lead

should be trained in Online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming

- cyber-bullying

Students / pupils:

- are responsible for using the *school / academy* digital technology systems in accordance with the Student / Pupil Acceptable User Policy

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the *school's* Online Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature*. Parents and carers will be encouraged to support the *school academy* in promoting good online practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- access to parents' sections of the website / Blog/ pupil records

- their children's personal devices in the school / academy (where this is allowed)

Community Users

Community Users who access school systems / website / Blog as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems

- Our E-Safety policy has been written by the Principal and It has been approved by governors.
- The E-Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Furthermore, to develop their Information Technology skills, pupils will learn about safe searches, filtering searches, creative commons when searching and using media and copywrite.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Firewalls and Global Proxy filter system are set for all school devices therefore applies when devices go home.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Email accounts are setup by school and monitored by school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work via school Blog, Website or Twitter.

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
  - Pupils' full names will not be used anywhere on the Website, Blog or Twitter, particularly in association with photographs.
  - Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- The staff at school will maintain the school Twitter and Blog account allowing The Olive Tree Primary School to share pupil learning and experiences with parents, community and the wider world. This gives pupils access to experts, access to first hand research and gives them an audience to share learning with.

Managing filtering

- The school will work with the technical support provider (Computeam) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Computing Lead and Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Weekly suspicious search reports will be sent to the Computing Lead and Headteacher to monitor.

Managing videoconferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call/Facetime/Skype.
- Videoconferencing/Facetime/Skype will be appropriately supervised for the pupils' age.

Mobile Technology

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils or parents is required.
- Mobile Technology (iPads) are used to support, enhance and transform teaching and learning in the classroom. Students are part of the 1:1 Family iPad programme which allows them to continue learning beyond school time-flipped Learning.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign an 'Acceptable ICT Use Agreement' before using any school IT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with direct supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Handling e-safety complaints

- A senior member of staff will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to E-Safety.

Communications Policy

Introducing the E-Safety policy to pupils

- School will continue to address and educate pupils on E-Safety with termly Assemblies, Safer Internet Days and PSCHE. Educating our pupils on E-Safety and keeping safe online is a whole responsibility not just that of the Computing Lead.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will sign a user agreement setting out the rules for the use of IT in and out of school.

Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained. There will be a staff induction and training on E-Safety including Radicalisation.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Website.

F Choudry

Principal

Updated: February 2017

Next Review: February 2018